

REMARKS

Applicant respectfully requests reconsideration of the rejection of this application as examined pursuant to the office action of April 26, 2005. In the office action, Claims 19-36 were examined. Claims 19-36 remain pending after entry of this amendment.

Claims 19-24, 26-28, and 30-36 were rejected under 35 USC § 102(e) as being anticipated by US Patent No. 6,871,287 issued to Ellingson. However, in the substantive portion of paragraph 3 of the office action, reference is only made to Tibor. A telephone conversation between Applicant's representative and the examiner, Mr. Kindred, confirmed that the appropriate citation in the rejection of Claims 19-24, 26-28, and 30-36 under 35 USC § 102(e) is to the published application of Tibor (US Publication No. 2004/0234117). Further in the office action, Claims 25 and 29 were rejected under 35 USC § 103(a) as being unpatentable over Tibor in view of Tibor. Confirmation was also obtained in the noted telephone conversation that the 35 USC § 103(a) rejection of Claims 25 and 29 was based on Tibor in view of Ellingson.

Applicant's claim amendments and arguments presented herein are based upon the understanding that Tibor is the primary reference relied upon by the examiner in rejecting the pending claims, whereas the Ellingson reference was relied upon solely in support of the Tibor reference with respect to Claims 25 and 29.

Applicant has taken this opportunity to amend independent pending Claims 19 and 26 of the application to distinguish the present invention with clarity in regard to the cited references. Specifically, Claim 19 has been amended to describe the persistent scanning step seeking indicia of misuse or error in the private information of the novel method of the invention as capable of being performed "without requiring initiation of the scanning through an action of the one or more individuals." That is, the present invention performs the scanning automatically, not solely in response to some action by the individual, such as attempting to verify a funds transfer transaction, for example. Similarly, Claim 26 has been amended to describe the means for comparing the known private information of the first database with the stored private information of the second database of the novel protection system of the invention as capable of being activated "without initiation through an action by the one or more individuals." Applicant respectfully suggests that the noted amendments to the independent claims are fully supported by the specification and further distinguish the present invention from the cited references.

The 35 USC § 102(e) Rejection

In the April 26, 2005, office action, Claims 19-24, 26-28, and 30-36 were rejected under 35 USC § 102(e) based on Tibor. Applicant has amended Claims 19 and 26 in a manner that further distinguishes the present invention from the transaction verification system described in the Tibor reference. Further, Applicant respectfully suggests that Tibor is directed to a system completely unrelated to the present invention. Yet further, Applicant respectfully suggests that Tibor should not have been cited in this matter as a substantial portion of the text therein relied upon in the office action was first made subject of the published application upon the continuation-in-part filing made April 1, 2004, nearly four years after the filing of the present application.

Claims 19 and 26 of the present application have been amended herein to note specifically that the protection method and system check for inaccurate individual private information contained in one or more databases, unauthorized use of individual private information retained in one or more database, or a combination of the two, occurs without any initiation by the individual. Once the individual first signs up to participate in the protection system and provides relevant private information, no further action is required on that person's part for the protection activities to occur. The system scans the one or more databases for the individual's private information, replicates any discovered information to a secured database, and compares the discovered information with the known information. Upon detecting any indicia of inaccuracy or misuse, the present invention addresses the problem, notifies the individual and/or authorized others about the problem, or a combination of the two. The individual does not have to initiate a transaction for the system to scan for inaccuracies or misuse. The amendments made to Claims 19 and 26 make that aspect of the invention clear.

On the other hand, the Tibor reference describes an electronic transaction verification system, not a persistent private information protection system of the type described by the present invention. As stated in paragraph [0011] of Tibor:

The present invention, in its simplest form, combines the use of valid biometric samples obtained from authentic identifications (IDs) with biometric samples provided by a person at a transaction location, thereby verifying that the biometric information presented for a transaction is a valid biometric for a particular person. In addition, the ID and the biometric sample can also be checked against known invalid users. Although it is possible for someone to counterfeit what is believed to be the authentic ID, in such cases, the identity thief provides an actual

fingerprint that has been taken and placed on the token or on the transaction slip. When the token is returned to the transaction location as forged, counterfeit, stolen, etc., the fingerprint is entered into the database of known invalid users, thus preventing any further identity theft activity by this person on the verification system. The present invention, in its most complex form, adds additional safeguards, such as verifying the ID with information from the state. This ensures that an ID has not been altered, and is in fact an authentic state-issued ID (e.g., driver's license). Another such safeguard is verifying the information at the processing center of the token with the original information that a bank or token company obtained at the creation of the bank or token account. (Emphasis added.)

Tibor requires that a person: a) provide a biometric sample; b) present that sample at a transaction location; and c) submit a token or a transaction slip in association with an intended transaction. The Tibor system then transmits the obtained biometric sample, such as a fingerprint, to a database for comparison to a known digitized version of the biometric sample. If there is a match, the transaction is approved and may proceed. If there is no match, the transaction may be denied, and the occurrence may be cataloged. Tibor simply provides a mechanism for protection, primarily, of a merchant by improving the opportunity to deny transfer of money, goods, etc., to an unauthorized individual. On the other hand, the present invention is designed primarily to protect the individual and, indirectly, those who lawfully retain the individual's private information in their databases. The present invention does not require a transaction event initiated by the individual to trigger a biometric sample matching event. Instead, the present invention scans for inaccurate private information or misused private information and acts upon detecting such inaccuracy or misuse. Claims 19 and 26 have been amended to clarify that distinction.

Applicant also notes that the published application of Tibor was filed on April 1, 2004, as a continuation-in-part of the application serial no. 09/335,649, filed June 18, 1999, now US Patent No. 6,728,397 (the '397 patent). Applicant's representative has reviewed the published application and compared the text thereof with the text of the '397 patent. Firstly, it is to be noted that the '397 patent was clearly directed solely to the concept of verifying a negotiable instrument, a check more particularly, offered at a point of sale. Secondly, many of the sections of the Tibor published application cited in paragraph 3 of the April 26, 2005, office action were modified from their corresponding sections of the '397 patent. For example, paragraph [0011] of the Tibor reference was not in the '397 patent. Paragraph [0012] of the Tibor reference,

corresponding to column 1, line 64, to column 2, line 14, of the '397 patent, includes additional and expanded descriptions of the information scanned from the negotiable instrument and data transfer. Paragraph [0030] of the Tibor reference, corresponding to column 3, line 65 to column 4, line 20, of the '397 patent, includes additional and expanded descriptions of the "identification database." Paragraph [0034] of the Tibor reference, corresponding to column 5, lines 25-37, of the '397 patent, includes additional and expanded descriptions of the processing of data and the information contained in the database. The '397 patent makes no mention in that section of the patent to a plurality of databases as described in paragraph [0035] of the Tibor reference.

In addition to the substantial differences between the published Tibor application cited and the '397 patent containing lesser information, Applicant respectfully suggests that the reference fails to teach one or more of the components that the April 26, 2005, office action indicates are taught. Specifically, it is stated in paragraph 3 of the office action that Tibor teaches "... persistently scanning one or more network communication systems for indicia (see paragraph [0030] and [0035]) ..." However, a review of the noted sections of the Tibor reference makes clear that Tibor provides no such teaching. Paragraph [0030] of the Tibor reference states:

Referring now in greater detail to the drawings, in which like numerals represent like components throughout the several views, FIG. 1 illustrates a block diagram of an exemplary embodiment of the verification system illustrating an electronic transaction verification unit 10 in communication with a central processing system 12 that includes an identification database 14. The identification database can include a number of databases used in the identification process such as a biometric database of known customer data, as well as a separate database of known invalid users. The database of known invalid users can be established by correlating a biometric presented at a transaction location that is used with a fraudulently obtained transaction token, and storing the biometric as invalid. Central processing system 12 can be a main system remote from the transaction location. While a check is disclosed as one type of token to be processed in an exemplary embodiment of the present inventive system, other tokens can be processed in the same manner as disclosed herein. Negotiable instrument, as the term is used herein is defined in Article 3 .sctn.104 of the Uniform Commercial Code. An instrument is negotiable if it is: (1) a written instrument signed by the endorser or maker; (2) an unconditional promise to pay a certain amount of money, either on demand or at a future date; and (3) payable to the holder or bearer. Examples of negotiable instruments are checks, bills of exchange, and promissory notes. A check as used herein means a draft, payable on demand and drawn on a bank, or a cashier or teller's check. This is the customary definition of a check. The exemplary embodiment of the electronic transaction verification unit

10 is comprised of, at least, a check scanner or token reader 16 and a biometric data-gathering device 18, such as a fingerprint recording device.

Nowhere in paragraph [0030] of the Tibor reference is there any mention of “persistently scanning” (Claim 19 of the present application) or “persistently searching” (Claim 26 of the present application) one or more databases that may contain private information for the purpose of relating that information with known private information. Paragraph [0030] further makes clear that Tibor only reviews its own known customer data or a database of invalid users when initiated by a transaction occurring through an action of an individual, namely, the attempt to conduct some form of funds transaction. Tibor would not detect an error in private information contained in a database, including a legitimate database. Tibor would not move to detect, for example, the storage of an individual’s credit card information stored in an unauthorized database unless and until a transaction was initiated. The present invention, on the other hand, persistently checks databases for the individual’s private information and, if determined to have defined indicia, such as unauthorized storage of the credit card number, the individual would be notified before an unauthorized transaction is initiated that such unauthorized storage exists. Preventive action may then be undertaken, rather than corrective action.

Similarly, paragraph [0035] of the Tibor reference fails to describe the persistent scanning or searching. Paragraph [0035] states:

At the central database 30, the incoming data is compared, either in parallel with or separately with token identification data, with the existing known data for authorized users of accounts, shown by decision block 32, and an approval is made as to whether or not to accept the token. Either a yes decision 34 or a no decision 36 on approval is then re-transmitted back to the computer hardware platform 28 of the check verification unit 10. While the check verification unit 10 is shown in communication with a database 30 remotely located thereto, it is not necessary that the central system 12 or the database 30 be located remotely to the electronic transaction verification unit 10. In fact, the electronic transaction verification unit 10 and central system 12 can be self-contained at the transaction location whereby the central database, or the account information and biometric databases are continually updated within the electronic transaction verification unit 10 through either a data connection to a master database or through periodic manual updates from storage media such as floppy disks or CD ROMs. In such an embodiment, the electronic transaction verification system is preferably self-contained and includes all the necessary devices for scanning drivers’ licenses 20, gathering biometric data (e.g., fingerprints) 18, or scanning checks/reading tokens 16 (gathering check or token information data) within one unit comprising the system.

Nowhere in paragraph [0035] of the Tibor reference is there any mention of “persistently scanning” (Claim 19 of the present application) or “persistently searching” (Claim 26 of the present application) one or more databases that may contain private information for the purpose of relating that information with known private information. Paragraph [0035] makes reference to “continually updated,” but that is only in respect to the relationship between the central database or account and biometric databases, and the master database. Nowhere in paragraph [0035] is it suggested that any database not under direct control of the system is persistently scanned or searched for the individual’s private information. Instead, it is likely that updating in respect of a particular individual’s information is only triggered as a result of a transaction. The present invention, on the other hand, persistently checks databases, including ones not under the system’s direct control, for the individual’s private information. Upon determination that detected information varies with known information, the individual is notified, the error corrected, or a combination of the two.

In view of the amendments made to independent Claims 18 and 26 and the arguments presented herein, Applicant respectfully suggests that the 35 USC § 102(e) rejection of pending Claims 19-24, 26-28 and 30-36 based on the Tibor reference published on a continuation-in-part application filed April 1, 2004, has been successfully traversed. Withdrawal of that rejection is therefore requested.

The 35 USC § 103(a) Rejection

In the April 26, 2005, office action, Claims 25 and 29 were rejected under 35 USC § 103(a) based on Tibor in view of Ellingson. Claims 25 and 29 are dependent upon independent Claims 19 and 26, respectively, which claims were amended as noted hereinabove. Applicant incorporates herein by reference the arguments presented above with respect to the Tibor reference. Further, Ellingson provides no indication of a system for persistently scanning or searching databases for private information as it relates to known private information, and doing such scanning or searching without first requiring a triggering action by an individual. Ellingson appears to be solely relied upon as teaching the concept of internet search engines, such as Yahoo, Google, etc. The present invention as claimed in the noted claims is directed to an identity theft protection system employing such search engines. The search engines alone are

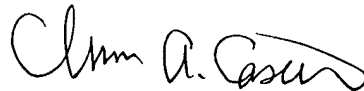
not claimed. Yet further, Tibor does not teach or fairly suggest relying upon Ellingson to teach such scanning or searching steps or arrangements. In view of the amendments made to independent Claims 19 and 26, and the arguments presented herein regarding Tibor and Ellingson, Applicant respectfully suggests that the 35 USC § 103(a) rejection of dependent Claims 25 and 29 has been successfully traversed. Withdrawal of that rejection is therefore requested.

CONCLUSION

In view of the amendments made to the independent claims and the arguments presented herein, Applicant respectfully suggests that the presently pending claims clearly describe the present invention and distinguish it over the cited Tibor and Ellingson references. It is therefore requested that this application be allowed to pass to issuance.

Applicant notes that no new claims have been added by this amendment. Therefore, no additional filing fee is required.


Respectfully submitted,



Chris A. Caseiro, Reg. No. 34,304
Attorney for Applicant
Verrill Dana, LLP
One Portland Square
Portland, ME 04112-0586
Tel. No. 207-253-4530

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the US Postal Service in an envelope with sufficient postage as first class mail and addressed to Mail Stop Non-Fee Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on June 23, 2005. It is hereby requested that this communication be assigned a filing date of June 23, 2005.


Chris A. Caseiro